E-Mail in 2018

nikolai.furmanczak@gmail.com
OpenRheinRuhr 2018

Inhalt

- SPF, DKIM und DMARC
- IP und Domain Reputation
  - z.B.: Spamtraps , Warm-Up etc …

SPF

Sender Policy Framework

Sender Policy Framework (SPF)

From-Header

„Friendly-From-Header“

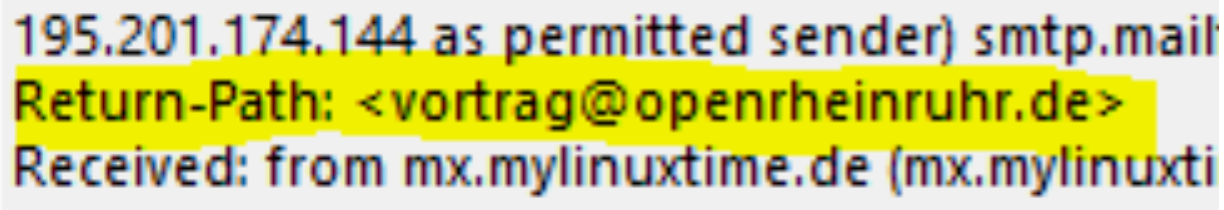
RFC 5322

Envelope-From

MAIL FROM SMTP-Handshake,

Return-Path

RFC 5321



Validierung SPF-Eintrag openrheinruhr.de

```
root@furmanczak:~# dig -t txt openrheinruhr.de +short
"v=spf1 mx -all"
```

Mechanismen:

- all
- ip4, ip6
- mx, a, aaaa
- include
- *uvm.*

Qualifikatoren:

- + Pass
- - (Hard)Fail
- ? Neutral
- ~ Softfail

SPF im DNS

```
root@furmanczak:~# dig -t txt openrheinruhr.de +short
"v=spf1 mx -all"
```

```
dig -t txt heise.de +short
"v=spf1 ip4:193.99.144.0/24 ip4:193.99.145.0/24 ip6:2a02:2e0:3fe:1001::/64
ip6:2a00:e68:14:800::/64 ip4:193.100.232.56 ip6:2a00:e68:14:801:bad::beef
include:spf.dynect.net include:_spf.intan.net  ip4:91.102.14.10  ip4:91.102.14.20
ip4:91.102.14.30 ?all"
```

```
dig -t txt spf.dynect.net +short
"v=spf1 ip4:208.76.56.0/21 ip4:216.146.32.0/20 -all"
```

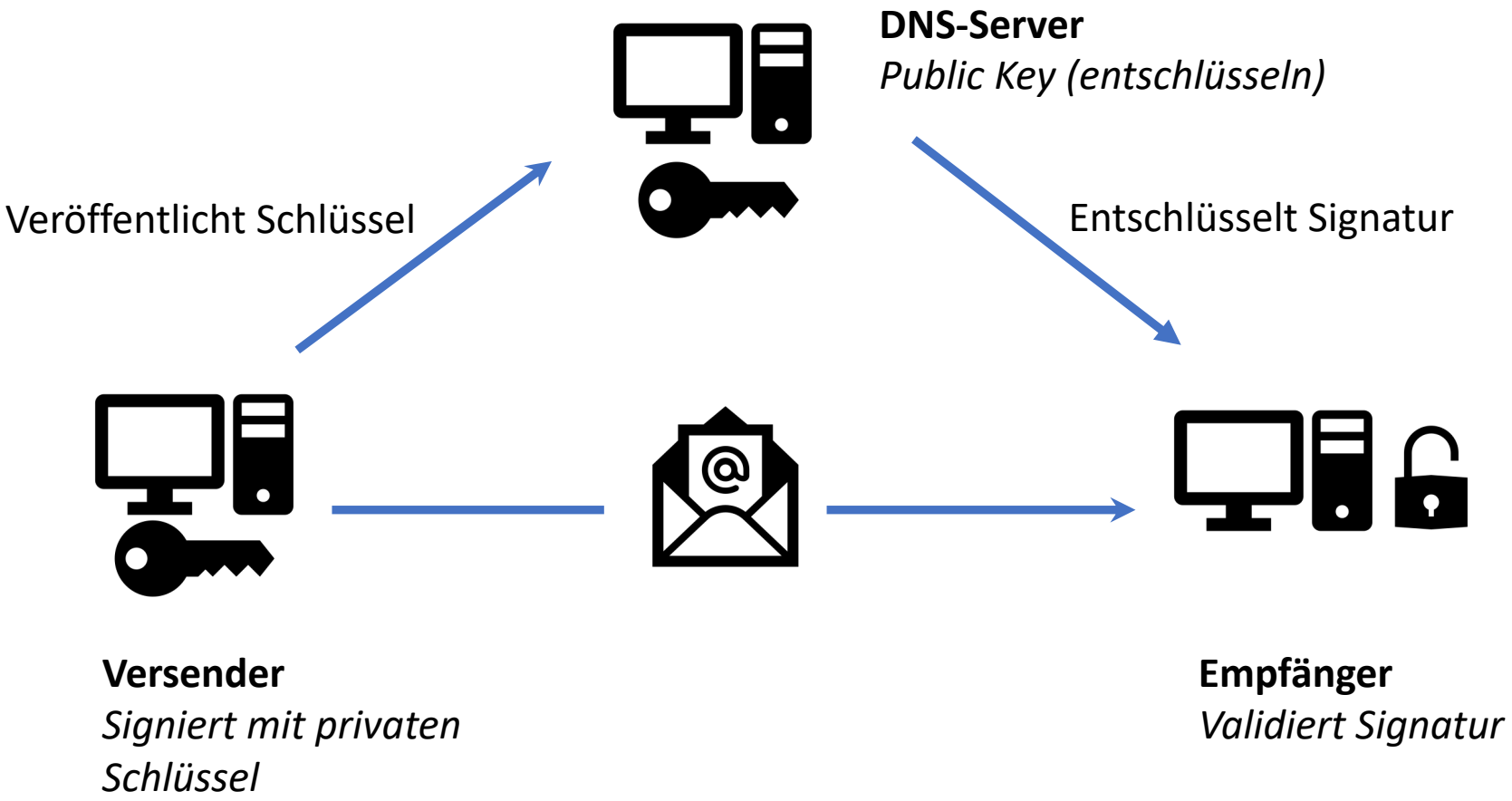
SPF – Gut zu wissen…

- SPF ist immer ein TXT-Eintrag (Typ SPF ist veraltet)
- SPF Record immer für envelop-from setzten
- Keine automatische Vererbung an Subdomains
- Gute Dokumentation nötig
- ?all oder ~all bei Einführung
- SPF auch möglich wenn keine E-Mails versenden werden v=spf1 -all

DKIM

DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM)



DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=furmanczak.de;
        s=201809; t=1539633028;
        bh=fdkeB/A0FkbVP2k4J4pNPoeWH6vqBm9+b0C3OY87Cw8=;
        h=Subject:To:Date:From:From;
        b=fPk6pqnw9CcUq89C2ESoG+NYH8l538E9Pr2bKG4yl9EVx4c96rkD1+zd9zbsk3n5V
         EBi0MJ04cQJa7A1eWPqZ6/yuUuQBJ7OlrL/poUAHI81JcCAIQuQxK1Hxtg0CDkWgxn
         yhg6qtAkJJpGZTkxbVUrcxX3HxlMZzppjSUXuZkA=
Subject: Test E-Mail
```

- bh=BASE64(SHA(Normalisierung(E-Mail Body)))
- b=BASE64(SHA(Normalisierung(E-Mail Header + DKIM-Signatur)))
- Signaturalgorithmen ~~SHA1~~, SHA2, RSA
- Selektor identifiziert Schlüssel (*selektor*._domainkey.example.org)

DKIM – Öffentlicher Schlüssel

```
dig -t txt 201809._domainkey.furmanczak.de +short
"v=DKIM1; h=sha256; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQK
BgQC6KN6G7Es3tiIj1wXIhGLu36besNY9XNV5VkG4HNF9YA9p+dTntKWr9Ay2VfW
dxruhUzopyrLWvJUnSe7zbfWl2m+GSf5ieMpDTESxkpj6iun6qEwsVUfc3ylw7C+
Cy7L/ZpcWQWCLRaeMLxTZb7j2PY0nQB7/4DJUdWV5y0zPMwIDAQAB"
```

DKIM – Gut zu wissen …

- Mehrere DKIM-Signaturen pro E-Mail möglich
- Signieren fehlender Header möglich
- Header doppelt signieren (over-signing)
- DKIM Alignment (DKIM Domain == From Domain)
- DKIM-Schlüssel alle 6 bis 12 Monate erneuern

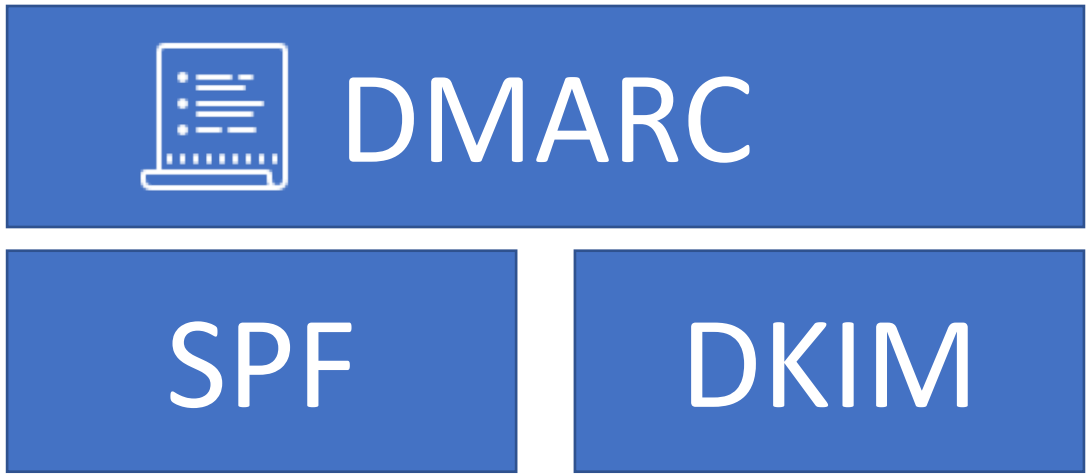
Tools für SPF und DKIM

- opendkim, dig
- DKIM Verifier (Thunderbird Plugin)
- dkimpy (Python), Mail::DKIM::Verifier (Perl)
- mxtoolbox.com, mail-tester.com

DMARC

Domain-based Message Authentication

DMARC als Regelwerk



- Schutz vor Missbrauch (z.B.: Phishing)
- Kontrolle der eigenen Infrastruktur
- DMARC *kann* auch ohne SPF und/oder DKIM genutzt werden

DMARC – DNS-Eintrag

Version	v=DMARC1;	
Policy (p,sp)	p=quarantine;	//reject, none
Traffic (%)	pct=100;	
Forensischer Report	rua=mailto:dmarc@domain.de;	
Aggregierter Report	ruf=mailto:forensik@domain.de;	
Regel DKIM	adkim=s;	//strict, relaxed
Regel SPF	aspf=r	//strict, relaxed

DMARC

- Starten mit p=none
- Regeln für SPF und DKIM zuerst relaxed
- Auf Datenflut einstellen (regulieren mittels pct)
- Tools zur Auswertung von DMARC (XML) Reports:
  - http://dmarc.postmarkapp.com
  - https://250ok.com/
  - https://www.fraudmarc.com/

Fazit

- SPF, DKIM, DMARC sind unsichtbar für Endbenutzer
- SPF, DKIM sind keine (zuverlässigen) SPAM Indikatoren
  - Empfehlung: Mindestens SPF mit ?all
- SPF, DKIM sind Vertrauensfaktoren für Mailboxprovider
- DNS-Server werden verstärktes Angriffsziel

Ausgangsszenario

Die Marketingabteilung möchte regelmäßig eure Kunden über neue Produkte, Aktionen, Veranstaltungen, etc … informieren.

1. Schritt: Technische Versandinfrastruktur

- Office E-Mail Server und Massen E-Mails (Newsletter oder Transactions E-Mails) trennen
- Reputation der IPv4 Adressen prüfen
  - Blacklisten (Spamhaus, Spamcop)
  - talosintelligence.com (ehemals senderbase.org)
  - returnpath.com

IP und Domain Reputation

Technisch

- DNS-Setup
- SPF, DKIM, DMARC
- DANE, DNSSec
- Sendevolumen
- AV-Scans, Mustererkennung, etc.
- Spamtraps
- Bounces

Userfeedback

- Beschwerden
- Öffnungsrate
- Lesedauer
- Spamklicks

1. Schritt: Technische Versandinfrastruktur

- Office E-Mail Server und Massen E-Mails (Bulk) trennen
- Reputation der IPv4 Adressen prüfen
  - Blacklisten (z.B.: Spamhaus, Spamcop)
  - talosintelligence.com (ehemals senderbase.org)
  - returnpath.com
- DNS-Setup
  - Reverse und Forward
  - Keine IP-Adresse im FQDN
  - Klassische TLD zum Versand (z.B: TLD .koeln vermeiden)
- SPF, DKIM und DMARC einrichten

2. Schritt: Anmeldeformular

- Double-Opt-In Verfahren (DOI, Gegenstück ist Single-Opt-In)
- Missbrauch der Formulare zum List-Bombing
  - Captcha
  - Begrenzung auf E-Mail Adressen/IP-Adresse
- Rückmeldung bei bereits angemeldeten E-Mail Adressen

2.1 Schritt: Bestehende Kontakte verwenden

Idee: Wir verwenden die Kontaktdaten aus unserem Kundensystem und beglücken alle unsere Kunden mit unseren neuem Newsletter.

Einwilligung für Werbezwecke zwingend erforderlich!
(Permissions Daten: E-Mail, IP, Datum, Uhrzeit)

Aber: Was ist mit bestehenden Kundenbeziehungen?

Schritt 3: Warum-Up Phase

- Traffic von neuen IP-Adressen langsam steigern
  - Zeitraum 3 bis 5 Wochen
  - Start ca. 10.000 E-Mails pro Woche
  - Pro Woche um +/- 15.000 E-Mails steigern
- Stark schwankenden Traffic vermeiden

Schritt 4: Listenhygiene und Spamtraps

- E-Mail Adressen mit bounces entfernen
- Sunsetting (Auslaufen von E-Mail Adressen)
- Monitoring und Feedback-Loops (FBL)
- Spamtraps:
  - Pristine
  - Recycled (Expired, Dead)
  - Typo

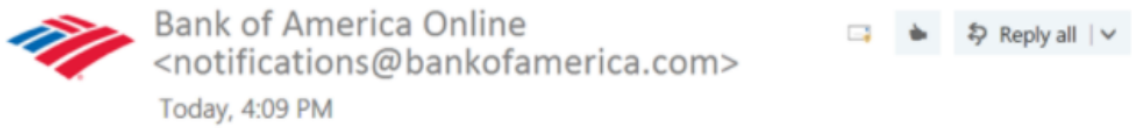
trustedDialog und BIMI

trustedDialog

Logo im Webclient
Teilnehmer: 1und1 (web.de,gmx.de), freenet, T-Online

BIMI

Brand Indicators for Message Identification



Logo außerhalb der E-Mail
(E-Mail Client oder Webinterface)
Aktuell wird BIMI und der Prozess noch diskutiert.

Dokumentation und Literatur

- Allgemeine Informationen zu SPF, DKIM und DMARC
  https://netplace.de/de/blog/dmarc
- Dokumentation DMARC
  https://www.msxfaq.de/spam/dmarc.htm
- Postfix + openDKIM Tutorial
  https://kofler.info/dkim-konfiguration-fuer-postfix/
- Exim + DKIM Tutorial
  https://www.exim.org/docs.html
- Exchange + DKIM Tutorial
  https://technet.microsoft.com/de-de/library/mt695945(v=exchg.150).aspx

Fragen?